Statement by South Africa at the Open-ended working group on security of and in the use of information and communications technologies 2021–2025 Informal Session held in March/April 2022 on promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats

- In a technology-driven world where governments and businesses are reliant on ICT systems for effective functioning, these systems have become critical infrastructure much like roads, hospitals, electricity grids, water infrastructure, telecommunications and financial systems. The increasing frequency, complexity and severity of cyber security incidents targeted at these critical systems, especially ransomware and hack-and-leak operations by criminal groups, State and non-State actors who seek to exploit post COVID-19 recovery initiatives, is a concern.

- From South Africa's perspective, it is important to build confidence and trust in the secure use of Information and Communication Technologies (ICTs), address security threats in cyberspace, combat cyber warfare, and develop, review and update existing substantive and procedural laws to ensure alignment.

- South Africa's initiatives aimed at ensuring security in the use of information and communications technologies include:

  - Enactment of the Cybercrimes Act 2021.
  - Enactment of the Protection of Personal Information Act (POPIA) in 2013. The Act came into force in July 2021.
  - Prioritisation of the review of the 2012 National Cybersecurity Strategy and the development of the National Cybersecurity Bill.
  - South Africa is cooperating both bilaterally and within like-minded groups to effectively address the rise in cybersecurity incidents such as ransomware, with the aim of reinforcing digital resilience, incident-response and skills development.

- It is essential at the national level to engage with private industry and civil society to create greater awareness of the risks and the urgency of addressing them. Engagement with national level stakeholders is an important component to promote transparency in the process. In South Africa's experience, a Cybersecurity Hub can be used as a mechanism for fostering public-private partnerships.

- It should be noted that while the threats to international security in the cyber realm are common, varying levels of risk based on varying national contexts exist and this needs to be taken into account in the development of practical measures to address these threats. Therefore, national level engagement needs to be the starting point to determining national priorities for areas of focus and international support.

- The challenge for governments in responding to these threats is that cyber-security activities need to be pursued across the whole of government, including sub-national levels such as provincial or local government, independent agencies, State owned enterprises and contractors, and in coordination with the private sector actors.

- At the international level, cooperation between States, including the development of norms and principles, is also a critical element for this OEWG in support of discussion towards a common understanding how international law applies to the cybersecurity, to ensure that the principle of State sovereignty and territorial integrity is maintained even in the context of cyberspace.